EVALUATION KIT AVAILABLE

MAXQ1103

DeepCover Secure Microcontroller with Rapid Zeroization Technology and Cryptography

General Description

DeepCover™ embedded security solutions cloak sensitive data under multiple layers of advanced physical security to provide the most secure key storage possible.

The DeepCover Secure Microcontroller (MAXQ1103) is a low-power, 32-bit RISC device that combines high-performance, single-cycle processing, sophisticated tamper-detection technology, and cryptographic hardware. Advanced security features are designed to meet the stringent requirements of regulations such as ITSEC E3 High, FIPS 140-2 Level 3, and the Common Criteria Certifications. The MAXQ1103 is targeted at electronic commerce, banking, and data security systems that require the highest levels of secure access control, secure data storage, digital signature, or certificate authentication. A secure memory protection unit protects critical internal and external memory against tampering with triple-DES (3DES) encryption. Activation of a tamper sensor causes a rapid zeroization of critical data. An internal physical shield layer increases the complexity and cost of a physical attack against the die.

A 32-bit MAXQ30 core powers the cryptographically secure MAXQ1103. Applications are supported with 512KB of high-performance internal flash memory for code/data storage and 32KB SRAM. Up to 8MB of additional external program and data memory is supported through a dedicated word-wide memory bus with programmable wait states. Additional peripherals such as serial I/O, 16-bit timers, hardware math accelerator, ISO 7816 UART, and a USB controller increase system utility while reducing component count.

System security is enhanced by the addition of high-speed cryptographic hardware accelerators for ECDSA, DSA, RSA, Secure Hash Algorithm, and triple-key 3DES. The embedded hash engine supports multiple hash functions recommended by the National Institute of Standards and Technology (NIST). The true hardware random-number generator (RNG) supports FIPS 186-2 with an available software library.

Applications

Electronic Commerce	Secure Access Control
PCI Terminals	Secure Data Storage
PIN Pads	Pay-per-Play
ATM Keyboards	Certificate Authentication
EMV® Banking	Electronic Signature Generator

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE	TAMPER RESPONSIVE
MAXQ1103-ENS+	-40°C to +85°C	144 TQFP	Yes

+Denotes a lead(Pb)-free/RoHS-compliant package.

Pin Configuration and Typical Application Circuit appear at end of data sheet.

DeepCover is a trademark and MAXQ is a registered trademark of Maxim Integrated Products, Inc.
EMV is a registered trademark of EMVCo, LLC.

Features

- **High-Performance 32-Bit MAXQ30 RISC Core**
- **DC to 25MHz Operation, Approaching 1MIPS per MHz**
- **Dual 1.8V Core/3.3V I/O Enables Low Power/ Flexible Interfacing**
- **5V Tolerant I/O**
- **Up to 32 General-Purpose I/O Pins**
- **34 Instructions, Most Single Cycle**
- **Three Independent Data Pointers Accelerate Data Movement with Automatic Increment/Decrement**
- **Virtually Unlimited Software Stack**
- **16-Bit Instruction Word, 32-Bit Internal Data Bus**
- **16 x 32-Bit Accumulators**
- **Security Features**
  - 3DES-Encrypted External Memory Bus Prevents Eavesdropping
  - Tamper Sensors Rapidly "Zeroize" Internal Keys and User Data When:
    - Out-of-Range Temperature/Voltage Detected
    - User-Defined Self-Destruct Inputs (SDIx) Activated
  - Internal Cryptographic Hardware Includes:
    - DES Engine Supporting Single DES and 2/3-Key 3DES Operations
    - Public-Key Cryptographic Accelerator for ECDSA (160-, 192-, and 256-Key Strength)
    - Public-Key Cryptographic Accelerator for DSA and RSA (1024- and 2048-Key Strength)
    - Hardware Hash Engine Supports SHA-1, SHA-224, and SHA-256
  - Unresettable True-Time Clock Self-Imposes Expiration Dates and Date/Timestamping
- **Memory Features**
  - Secure Memory Protection Unit and 4KB Instruction Cache
  - 512KB of Internal Flash Program Memory
  - 3KB Internal Program Memory SRAM
  - 32KB Internal Data SRAM, Including 1KB Battery-Backed NV SRAM
  - Linear Address Space Directly Accesses Up to 8MB of External Program/Data Memory
- **Peripheral Features**
  - USB Device Controller with Four Endpoint Buffers
  - ISO 7816 UART with FIFO with Two Physically Separate Communication Buses
- **Power Management Features**
- **In-System Programming Through Debug Port or Serial Port**
- **Ultra-Low Battery Leakage to Support NV RAM and Security Sensors (150nA)**

See the Detailed Features *section for complete list of features.*

Note: *Some revisions of this device may incorporate deviations from published specifications known as errata. Multiple revisions of any device may be simultaneously available through various sales channels. For information about device errata, contact the factory.*

For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim Integrated's website at www.maximintegrated.com.

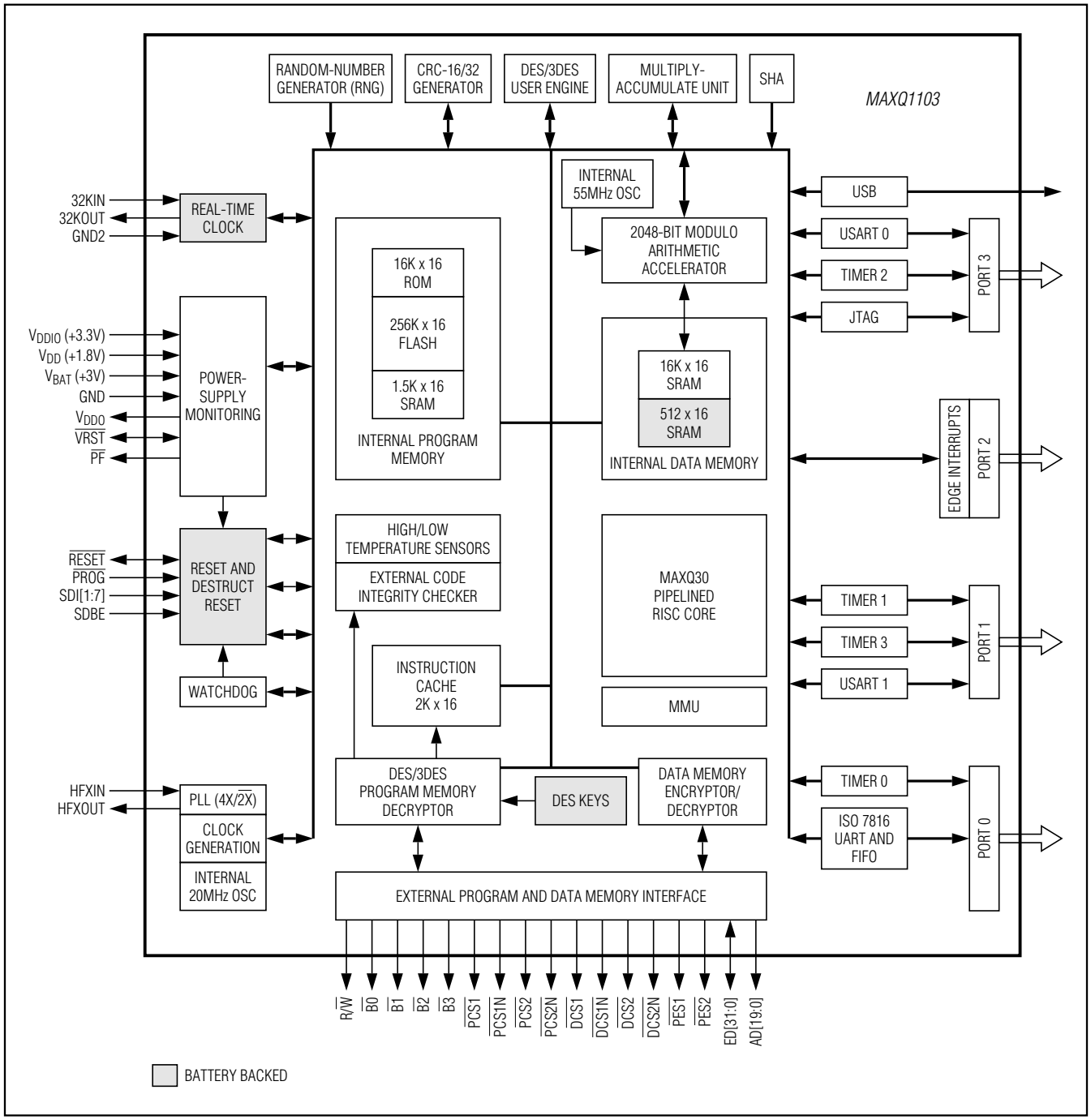
19-5091; Rev 5; 1/13

ABRIDGED DATA SHEET

MAXQ1103

DeepCover Secure Microcontroller with Rapid Zeroization Technology and Cryptography

Functional Diagram



Note to readers: This document is an abridged version of the full data sheet. To request the full data sheet, go to www.maximintegrated.com/MAXQ1103 and click on **Request Full Data Sheet**.